MS. THESIS

Secrecy Performance of Full-Duplex Relay System With Randomly Located Eavesdroppers

무작위로 위치한 다수 도청자가 존재하는 전이중 중계 시스템의 보안 성능

BY

Donghyun Jung

AUGUST 2017

DEPARTMENT OF ELECTRICAL AND
COMPUTER ENGINEERING
COLLEGE OF ENGINEERING
SEOUL NATIONAL UNIVERSITY

Abstract

Secrecy Performance of Full-Duplex Relay System With Randomly Located Eavesdroppers

Donghyun Jung

Department of Electrical and Computer Engineering

The Graduate School

Seoul National University

Full-duplex (FD) operation improves the spectral efficiency of a relay system where the relay simultaneously transmits and receives signals on the same channel. The performance of FD relay systems is limited by self-interference, i.e., signal leakage from the relay's transmit antenna to its receive antenna. However, in the FD relay system with malicious eavesdroppers, simultaneous transmission from the source and relay confuses the eavesdroppers.

In this thesis, we investigate a FD relay system where a source communicates with a destination via a decode-and-forward relay in the presence of randomly located eavesdroppers. We derive analytical expressions for the secrecy outage probability and the average secrecy rate of the system. Simulation results show that the secrecy performance of the system is improved as the density of eavesdroppers decreases. It is also shown that the FD relay system has higher secrecy performance than the half-duplex relay system when a large portion of self-interference is cancelled.

Keywords: Physical layer security, stochastic geometry, full-duplex relay system, randomly located eavesdroppers, secrecy outage probability, average secrecy rate.

Student Number: 2015-20987.

Contents

List of Figures

Chapter 1

Introduction

Full-duplex (FD) operation improves the spectral efficiency of a relay system where the relay simultaneously transmits and receives signals on the same channel [1]. However, the main limitation of the FD relay system is that simultaneous transmission and reception at the relay causes a high level of self-interference, i.e., signal leakage from the relay's transmit antenna to its receive antenna. Several techniques to mitigate the effect of the self-interference at FD nodes have been investigated, such as passive cancellation, analog cancellation, and digital cancellation [2]-[5].

Communication is secure when a legitimate receiver successfully decodes its received signal from a transmitter while an eavesdropper cannot overhear the signal. Physical layer security guarantees the secure communication by using the characteristics of wireless channels without encryption methods [6], [7]. The effects of malicious eavesdroppers who attempt to overhear the communication between the legitimate transmitter and receiver have been considered.

Randomly located eavesdroppers have been recently investigated where eavesdroppers' positions are modeled by using stochastic geometry [8]-[13]. In [8], secrecy performance of a downlink cellular system was analyzed where a multi-antenna base station communicates with multiple malicious users in the presence of external eavesdroppers. In [9], an artificial noise-aided multi-antenna transmission scheme was studied where optimal power allocation between an information signal and an artificial noise which minimizes the secrecy outage probability was obtained. In [10], secrecy performance of a downlink cellular system in the presence of randomly located eavesdroppers was analyzed where a multi-antenna base station employs transmit antenna

selection to enhance the secrecy performance. In [11], a secure transmission scheme in a half-duplex (HD) relay system was investigated where the source and relay transmit artificial noises along with information signals to confuse eavesdroppers.

In a FD relay system with an eavesdropper, simultaneous transmission from the source and relay confuses the eavesdropper [14]-[17]. In [14], a FD jamming relay system was proposed where the relay receives an information signal from the source and simultaneously transmits a jamming signal to the eavesdropper. In [15], a power allocation algorithm which maximizes the secrecy rate of the FD relay system was presented. In [16], the secrecy outage probability of a two-way FD relay system with optimal relay seletion was analyzed. In [17], an Almouti-based beamforming and artificial noise design was proposed to maximize the secrecy rate of the two-way FD relay system. However, most previous works focused on eavesdropper(s) at deterministic position(s) in the FD relay system.

In this thesis, we consider a FD relay system with randomly located eavesdroppers. We derive analytical expressions for the secrecy outage probability

and the average secrecy rate of the system. Computer simulations verify the validity of our analysis. Also, the performance of a HD relay system with randomly located eavesdroppers is compared with the FD relay system.

The rest of this thesis is organized as follows. In chapter 2, the system model is described. In chapter 3, the secrecy outage probability and the average secrecy rate are analyzed. In chapter 4, simulation results are provided. Finally, conclusions are drawn in chapter 5.

Chapter 2

System Model

Consider a FD relay system where a source s communicates with a destination d via a decode-and-forward (DF) relay r in the presence of multiple eavesdroppers. Assume that the source, the relay, and the destination are located at fixed positions and there is no direct link between the source and the destination. Assume that the eavesdroppers are located according to a homogeneous Poisson point process (PPP) Φ_e with density λ_e. Suppose that the FD relay has two antennas, one for transmission and one for reception while the source, the destination, and the eavesdroppers have a single

antenna.

Suppose that transmission takes place in blocks. In each block, the source transmits a signal to the relay and, at the same time, the relay transmits a signal to the destination. The relay receives not only the signal transmitted from the source but also the signal transmitted from itself which becomes interference. The relay decodes and re-encodes the received signal, and in the next block, transmits the re-encoded signal to the destination.

The eavesdroppers attempt to overhear the signals transmitted from the source and the relay. Suppose that the source and the relay use different codebooks, so that the eavesdroppers can only individually decode the received signal from the first hop and that from the second hop [11]. Assume that the eavesdroppers are non-colluding, i.e., each eavesdropper does not cooperate with other eavesdroppers [9].

Assume that all channels remain constant over a block and vary independently from one block to another. Assume that the coefficient of the channel from node i to node j in block k, $h_{ij}[k]$, $i, j \in \{s, r, d, e\}$, $e \in \Phi_e$, is an independent complex Gaussian random variable with zero mean and unit

variance. Assume that the channels have an additive white Gaussian noise (AWGN) with zero mean and variance N_0.

In block k, the source transmits a signal $x_s[k]$ with power P_s to the relay and the relay transmits the re-encoded signal of $x_s[k-1]$, denoted by $\hat{x}_s[k-1]$, with power P_r to the destination. Let ρ, $\rho \in [0,1]$, denote the self-interference cancellation factor which represents a residual portion of self-interference power at the relay after cancellation [5]. The received signal at the relay is given by

$$y_r[k] = \sqrt{d_{sr}^{-\alpha}} h_{sr}[k] x_s[k] + \sqrt{\rho} h_{rr}[k] \hat{x}_s[k-1] + n_r[k] \tag{2.1}$$

where d_{sr} is the distance from the source to the relay, α is the path-loss exponent, and $n_r[k]$ is an AWGN. The received signal at an eavesdropper (at position) e, $e \in \Phi_e$, is given by

$$y_e[k] = \sqrt{d_{se}^{-\alpha}} h_{se}[k] x_s[k] + \sqrt{d_{re}^{-\alpha}} h_{re}[k] \hat{x}_s[k-1] + n_e[k] \tag{2.2}$$

where d_{se} and d_{re} are the distance from the eavesdropper e to the source and

that to the relay, respectively, and $n_e[k]$ is an AWGN.

In block $k+1$, the received signal at the destination is given by

$$y_d[k+1] = \sqrt{d_{rd}^{-\alpha}} h_{rd}[k+1]\hat{x}_s[k] + n_d[k+1] \tag{2.3}$$

where d_{rd} is the distance from the relay to the destination and $n_d[k+1]$ is an AWGN. The received signal at the eavesdropper e is given by

$$\begin{aligned} y_e[k+1] =& \sqrt{d_{re}^{-\alpha}} h_{re}[k+1]\hat{x}_s[k] \\ &+ \sqrt{d_{se}^{-\alpha}} h_{se}[k+1]x_s[k+1] + n_e[k+1]. \end{aligned} \tag{2.4}$$

The signal-to-interference-plus-noise ratios (SINR) at the relay is given by

$$\gamma_{sr} = \frac{P_s d_{sr}^{-\alpha} |h_{sr}[k]|^2}{\rho P_r |h_{rr}[k]|^2 + N_0}. \tag{2.5}$$

The signal-to-noise ratio (SNR) at the destination is given by

$$\gamma_{rd} = \frac{P_r d_{rd}^{-\alpha} |h_{rd}[k+1]|^2}{N_0}. \tag{2.6}$$

For DF relaying, the end-to-end SINR from the source to the destination is given by

$$\gamma_d = \min\{\gamma_{sr}, \gamma_{rd}\}. \tag{2.7}$$

The SINR at the eavesdropper e for the signal transmitted from the source is given by

$$\gamma_{se} = \frac{P_s d_{se}^{-\alpha} |h_{se}[k]|^2}{P_r d_{re}^{-\alpha} |h_{re}[k]|^2 + N_0}. \tag{2.8}$$

The SINR at the eavesdropper e for the signal transmitted from the relay is given by

$$\gamma_{re} = \frac{P_r d_{re}^{-\alpha} |h_{re}[k+1]|^2}{P_s d_{se}^{-\alpha} |h_{se}[k+1]|^2 + N_0}. \tag{2.9}$$

Since the source and relay use different codebooks, the SINR at the eavesdropper e is given by [11]

$$\gamma_e = \max\{\gamma_{se}, \gamma_{re}\}. \tag{2.10}$$

For non-colluding eavesdroppers, the secrecy rate of the system is determined by the most detrimental eavesdropper, i.e., an eavesdropper with the highest

SINR which is given by

$$\gamma_{e^*} = \max_{e \in \Phi_e} \gamma_e. \tag{2.11}$$

Chapter 3

Secrecy Performance Analysis

In this chapter, we first analyze the cumulative distribution functions (CDFs) of γ_d and γ_{e^*}. Then, we derive analytical expressions for the secrecy outage probability and the average secrecy rate of the FD relay system.

3.1 SINR Distribution

The CDF of the end-to-end SINR from the source to the destination is given by

$$\begin{aligned} F_{\gamma_d}(x) =& \Pr[\gamma_d < x] \\ =& 1 - \Pr[\min\{\gamma_{sr}, \gamma_{rd}\} \geq x] \\ =& 1 - \Pr[\gamma_{sr} \geq x, \gamma_{rd} \geq x] \\ =& 1 - (1 - F_{\gamma_{sr}}(x))\,(1 - F_{\gamma_{rd}}(x)) \end{aligned} \tag{3.1}$$

where $F_{\gamma_{sr}}(x)$ and $F_{\gamma_{rd}}(x)$ are the CDFs of γ_{sr} and γ_{rd}, respectively. The CDF of the SINR at the relay is given by

$$\begin{aligned} F_{\gamma_{sr}}(x) =& \Pr[\gamma_{sr} < x] \\ =& \Pr\left[\frac{P_s d_{sr}^{-\alpha} U}{\rho P_r V + N_0} < x\right] \\ =& \Pr\left[U < \frac{\rho P_r V + N_0}{P_s d_{sr}^{-\alpha}} x\right] \\ =& \int_0^{\infty} \int_0^{\frac{\rho P_r v + N_0}{P_s d_{sr}^{-\alpha}} x} f_{U,V}(u,v)\,du\,dv \end{aligned} \tag{3.2}$$

where $U = |h_{sr}[k]|^2$, $V = |h_{rr}[k]|^2$, and $f_{U,V}(u,v)$ is the joint probability density function (PDF) of U and V. Since U and V are independent exponential random variables with unit mean, we have

$$\begin{aligned}
F_{\gamma_{sr}}(x) &= \int_0^{\infty} \int_0^{\frac{\rho P_r v + N_0}{P_s d_{sr}^{-\alpha}} x} f_U(u) f_V(v) du dv \\
&= \int_0^{\infty} \exp(-v) \int_0^{\frac{\rho P_r v + N_0}{P_s d_{sr}^{-\alpha}} x} \exp(-u) du dv \\
&= \int_0^{\infty} \exp(-v) \left(1 - \exp\left(-\frac{\rho P_r v + N_0}{P_s d_{sr}^{-\alpha}} x\right)\right) dv \\
&= 1 - \exp\left(-\frac{N_0 d_{sr}^{\alpha}}{P_s} x\right) \int_0^{\infty} \exp\left(-\left(1 + \frac{\rho P_r d_{sr}^{\alpha}}{P_s} x\right) v\right) dv \\
&= 1 - \exp\left(-\frac{N_0 d_{sr}^{\alpha}}{P_s} x\right) \left(1 + \frac{\rho P_r d_{sr}^{\alpha}}{P_s} x\right)^{-1}
\end{aligned} \tag{3.3}$$

where $f_U(u)$ and $f_V(v)$ are the PDFs of U and V, respectively. The CDF of the SNR at the destination is given by

$$
\begin{aligned}
F_{\gamma_{rd}}(x) =& \Pr[\gamma_{rd} < x] \\
=& \Pr\left[|h_{rd}[k+1]|^2 < \frac{N_0 d_{rd}^{\alpha}}{P_r} x\right] \\
=& 1 - \exp\left(-\frac{N_0 d_{rd}^{\alpha}}{P_r} x\right)
\end{aligned} \tag{3.4}
$$

where $|h_{rd}[k+1]|^2$ has an exponential distribution with unit mean. From (3.1), (3.3), and (3.4), the CDF of the end-to-end SINR from the source to the destination is obtained as

$$
F_{\gamma_d}(x) = 1 - \exp\left(-N_0\left(\frac{d_{sr}^{\alpha}}{P_s} + \frac{d_{rd}^{\alpha}}{P_r}\right)x\right)\left(1 + \frac{\rho P_r d_{sr}^{\alpha}}{P_s} x\right)^{-1}. \tag{3.5}
$$

The CDF of the SINR at the most detrimental eavesdropper is given by

$$
\begin{aligned}
F_{\gamma_{e^*}}(x) =& \Pr[\gamma_{e^*} < x] \\
=& \mathbb{E}_{\Phi_e}\left[\prod_{e \in \Phi_e} \Pr[\max\{\gamma_{se}, \gamma_{re}\} < x]\right] \\
=& \mathbb{E}_{\Phi_e}\left[\prod_{e \in \Phi_e} \Pr[\gamma_{se} < x] \Pr[\gamma_{re} < x]\right]
\end{aligned}
$$

$$=\mathbb{E}_{\Phi_e}\left[\prod_{e\in\Phi_e} F_{\gamma_{se}}(x)F_{\gamma_{re}}(x)\right] \tag{3.6}$$

where $F_{\gamma_{se}}(x)$ and $F_{\gamma_{re}}(x)$ are the CDFs of γ_{se} and γ_{re}, respectively. Similarly to the derivation of (3.3), the CDF of the SINR at the eavesdropper e for the signal transmitted from the source is given by

$$F_{\gamma_{se}}(x) = 1 - \exp\left(-\frac{N_0 d_{se}^{\alpha}}{P_s}x\right)\left(1 + \frac{P_r}{P_s}\left(\frac{d_{se}}{d_{re}}\right)^{\alpha}x\right)^{-1} \tag{3.7}$$

and the CDF of the SINR at the eavesdropper e for the signal transmitted from the relay is given by

$$F_{\gamma_{re}}(x) = 1 - \exp\left(-\frac{N_0 d_{re}^{\alpha}}{P_r}x\right)\left(1 + \frac{P_s}{P_r}\left(\frac{d_{re}}{d_{se}}\right)^{\alpha}x\right)^{-1}. \tag{3.8}$$

From (3.6), (3.7), and (3.8), the CDF of the SINR at the most detrimental eavesdropper is obtained as

$$
\begin{aligned}
F_{\gamma_e}(x) =& E_{\Phi_e}\left[\prod_{e\in\mathcal{K}_e}\left(1-\exp\left(-\frac{N_0 d_{se}^{\alpha}}{P_s}x\right)\left(1+\frac{P_r}{P_s}\left(\frac{d_{se}}{d_{re}}\right)^{\alpha}x\right)^{-1}\right)\right.\\
&\left.\times\left(1-\exp\left(-\frac{N_0 d_{re}^{\alpha}}{P_r}x\right)\left(1+\frac{P_s}{P_r}\left(\frac{d_{re}}{d_{se}}\right)^{\alpha}x\right)^{-1}\right)\right]\\
\overset{(a)}{=}& \exp\left(-\lambda_e\int_0^{\infty}\int_0^{2\pi} d_{se}\left\{\exp\left(-\frac{N_0 d_{se}^{\alpha}}{P_s}x\right)\left(1+\frac{P_r}{P_s}\left(\frac{d_{se}}{d_{re}}\right)^{\alpha}x\right)^{-1}\right.\right.\\
&+\exp\left(-\frac{N_0 d_{re}^{\alpha}}{P_r}x\right)\left(1+\frac{P_s}{P_r}\left(\frac{d_{re}}{d_{se}}\right)^{\alpha}x\right)^{-1}\\
&-\exp\left(-N_0\left(\frac{d_{se}^{\alpha}}{P_s}+\frac{d_{re}^{\alpha}}{P_r}\right)x\right)\left(1+\frac{P_r}{P_s}\left(\frac{d_{se}}{d_{re}}\right)^{\alpha}x\right)^{-1}\\
&\left.\left.\times\left(1+\frac{P_s}{P_r}\left(\frac{d_{re}}{d_{se}}\right)^{\alpha}x\right)^{-1}\right\}d\theta d d_{se}\right.\\
\overset{(b)}{=}& \exp\left(-\lambda_e\int_0^{\infty}\int_0^{2\pi} d_{se}\left\{\exp\left(-\frac{N_0 d_{se}^{\alpha}}{P_s}x\right)\right.\right.\\
&\times\left(1+\frac{P_r}{P_s}\left(\frac{d_{se}}{\sqrt{d_{sr}^2+d_{se}^2-2d_{sr}d_{se}\cos\theta}}\right)^{\alpha}x\right)^{-1}\\
&+\exp\left(-\frac{N_0\sqrt{d_{sr}^2+d_{se}^2-2d_{sr}d_{se}\cos\theta}^{\alpha}}{P_r}x\right)\\
&\times\left(1+\frac{P_s}{P_r}\left(\frac{\sqrt{d_{sr}^2+d_{se}^2-2d_{sr}d_{se}\cos\theta}}{d_{se}}\right)^{\alpha}x\right)^{-1}\\
&\left.\left.-\exp\left(-N_0\left\{\frac{d_{se}^{\alpha}}{P_s}+\frac{\sqrt{d_{sr}^2+d_{se}^2-2d_{sr}d_{se}\cos\theta}^{\alpha}}{P_r}\right\}x\right)\right.
\end{aligned}
$$

$$\times \left(1+\frac{P_r}{P_s}\left(\frac{d_{se}}{\sqrt{d_{sr}^2+d_{se}^2-2d_{sr}d_{se}\cos\theta}}\right)^{\alpha}x\right)^{-1}$$
$$\times \left(1+\frac{P_s}{P_r}\left(\frac{\sqrt{d_{sr}^2+d_{se}^2-2d_{sr}d_{se}\cos\theta}}{d_{se}}\right)^{\alpha}x\right)^{-1}\Bigg\} d\theta dd_{se}\Bigg) \quad (3.9)$$

where (a) follows by using the probability generating functional of the PPP Φ_e which is given by [18]

$$\mathbb{E}_{\Phi_e}\left[\prod_{x\in\Phi_e} f(x)\right] = \exp\left(-\lambda_e \int_{\mathbb{R}^2} (1-f(x))dx\right) \quad (3.10)$$

and by changing to the polar coordinates, and (b) follows from the law of cosines, i.e., $d_{re} = \sqrt{d_{sr}^2+d_{se}^2-2d_{sr}d_{se}\cos\theta}$.

3.2 Secrecy Outage Probability

The secrecy rate of the system is given by

$$R = [\log(1+\gamma_d) - \log(1+\gamma_{e^*})]^+ \quad (3.11)$$

where $[x]^+ \triangleq \max\{0, x\}$. The secrecy outage probability of the system is given by [12]

$$\begin{aligned} P_{\text{out}} =& \Pr[R \leq 0] \\ =& \Pr[\log(1+\gamma_d) - \log(1+\gamma_{e^*}) \leq 0] \\ =& \Pr[\gamma_d \leq \gamma_{e^*}] \\ =& \int_0^\infty \int_x^\infty f_{\gamma_d}(x) f_{\gamma_{e^*}}(y) dy dx \\ =& 1 - \int_0^\infty f_{\gamma_d}(x) F_{\gamma_{e^*}}(x) dx \end{aligned} \tag{3.12}$$

where $f_{\gamma_d}(x)$ and $f_{\gamma_{e^*}}(y)$ are the PDFs of γ_d and γ_{e^*}, respectively. The PDF of the end-to-end SINR from the source to the destination is given by

$$\begin{aligned} f_{\gamma_d}(x) =& \frac{dF_{\gamma_d}(x)}{dx} \\ =& -\frac{d}{dx}\left\{ \exp\left(-N_0 \left(\frac{d_{sr}^\alpha}{P_s} + \frac{d_{rd}^\alpha}{P_r} \right) x \right) \left(1 + \frac{\rho P_r d_{sr}^\alpha}{P_s} x \right)^{-1} \right\} \\ =& \exp\left(-N_0 \left(\frac{d_{sr}^\alpha}{P_s} + \frac{d_{rd}^\alpha}{P_r} \right) x \right) \left(1 + \frac{\rho P_r d_{sr}^\alpha}{P_s} x \right)^{-1} \\ & \times \left(N_0 \left(\frac{d_{sr}^\alpha}{P_s} + \frac{d_{rd}^\alpha}{P_r} \right) + \left(\frac{P_s}{\rho P_r d_{sr}^\alpha} + x \right)^{-1} \right). \end{aligned} \tag{3.13}$$

From (3.9), (3.12), and (3.13), the secrecy outage probability is obtained as

$$
\begin{aligned}
P_{\text{out}} =& 1 - \int_0^{\infty} \left(1 + \frac{\rho P_r d_{sr}^{\alpha}}{P_s} x\right)^{-1} \left(N_0 \left(\frac{d_{sr}^{\alpha}}{P_s} + \frac{d_{rd}^{\alpha}}{P_r}\right) + \left(x + \frac{P_s}{\rho P_r d_{sr}}\right)^{-1}\right) \\
& \times \exp\left(-N\left(\frac{d_{sr}^{\alpha}}{P_s} + \frac{d_{rd}^{\alpha}}{P_r}\right) x - \lambda_e \int_0^{\infty} \int_0^{2\pi} d_{se} \left\{ \exp\left(-\frac{N_0 d_{se}^{\alpha}}{P_s} x\right) \right.\right. \\
& \times \left(1 + \frac{P_r}{P_s}\left(\frac{d_{se}}{\sqrt{d_{sr}^2 + d_{se}^2 - 2 d_{sr} d_{se} \cos\theta}}\right)^{\alpha} x\right)^{-1} \\
& + \exp\left(-\frac{N_0 \sqrt{d_{sr}^2 + d_{se}^2 - 2 d_{sr} d_{se} \cos\theta}^{\alpha}}{P_r} x\right) \\
& \times \left(1 + \frac{P_s}{P_r}\left(\frac{\sqrt{d_{sr}^2 + d_{se}^2 - 2 d_{sr} d_{se} \cos\theta}}{d_{se}}\right)^{\alpha} x\right)^{-1} \\
& - \exp\left(-N_0 \left(\frac{d_{se}^{\alpha}}{P_s} + \frac{\sqrt{d_{sr}^2 + d_{se}^2 - 2 d_{sr} d_{se} \cos\theta}^{\alpha}}{P_r}\right) x\right) \\
& \times \left(1 + \frac{P_r}{P_s}\left(\frac{d_{se}}{\sqrt{d_{sr}^2 + d_{se}^2 - 2 d_{sr} d_{se} \cos\theta}}\right)^{\alpha} x\right)^{-1} \\
& \left.\left. \times \left(1 + \frac{P_s}{P_r}\left(\frac{\sqrt{d_{sr}^2 + d_{se}^2 - 2 d_{sr} d_{se} \cos\theta}}{d_{se}}\right)^{\alpha} x\right)^{-1} \right\} d\theta d d_{se} \right) dx.
\end{aligned}
\tag{3.14}
$$

3.3 Average Secrecy Rate

The average secrecy rate of the system is given by [19]

$$\begin{aligned} R_{\text{avg}} =& \mathbb{E}[R] \\ =& \frac{1}{\ln 2}\int_0^\infty \frac{F_{\gamma_{e^*}}(x)}{1+x}(1-F_{\gamma_d}(x))dx. \end{aligned} \tag{3.15}$$

From (3.5), (3.9), and (3.15), the average secrecy rate is obtained as

$$\begin{aligned} R_{\text{avg}} =& \frac{1}{\ln 2}\int_0^\infty (1+x)^{-1}\left(1+\frac{\rho P_r d_{sr}}{P_s}x\right)^{-1} \\ & \times \exp\left(-N_0\left(\frac{d_{sr}^\alpha}{P_s}+\frac{d_{rd}^\alpha}{P_r}\right)x - \lambda_e\int_0^\infty\int_0^{2\pi} d_{se}\left\{\exp\left(-\frac{N_0 d_{se}^\alpha}{P_s}x\right)\right.\right. \\ & \times \left(1+\frac{P_r}{P_s}\left(\frac{d_{se}}{\sqrt{d_{sr}^2+d_{se}^2-2d_{sr}d_{se}\cos\theta}}\right)^\alpha x\right)^{-1} \\ & + \exp\left(-\frac{N_0\sqrt{d_{sr}^2+d_{se}^2-2d_{sr}d_{se}\cos\theta}^\alpha}{P_r}x\right) \\ & \times \left(1+\frac{P_s}{P_r}\left(\frac{\sqrt{d_{sr}^2+d_{se}^2-2d_{sr}d_{se}\cos\theta}}{d_{se}}\right)^\alpha x\right)^{-1} \\ & - \exp\left(-N_0\left(\frac{d_{se}^\alpha}{P_s}+\frac{\sqrt{d_{sr}^2+d_{se}^2-2d_{sr}d_{se}\cos\theta}^\alpha}{P_r}\right)x\right) \\ & \times \left.\left.\left(1+\frac{P_r}{P_s}\left(\frac{d_{se}}{\sqrt{d_{sr}^2+d_{se}^2-2d_{sr}d_{se}\cos\theta}}\right)^\alpha x\right)^{-1}\right\}\right. \end{aligned}$$

$$\times \left(1 + \frac{P_s}{P_r} \left(\frac{\sqrt{d_{sr}^2 + d_{se}^2 - 2d_{sr}d_{se}\cos\theta}}{d_{se}} \right)^{\alpha} x \right)^{-1} \Bigg\} d\theta dd_{se} \Bigg) dx. \tag{3.16}$$

Closed-form expressions of (3.14) and (3.16) are difficult to obtain, but they can be computed by using Gaussian quadrature method or software such as Mathematica [11]-[13].

Chapter 4

Simulation Results

Consider a FD relay system which consists of a source, a DF relay, a destination, and multiple eavesdroppers. Suppose that the path-loss exponent $\alpha = 4$, the distances from the source to the relay and from the relay to the destination $d_{sr} = d_{rd} = 10$ m, and the transmit SNRs of the source and relay $P_s/N_0 = P_r/N_0 = P/N_0$. In figures 4.1, 4.2, 4.5, and 4.6, the performance of a HD relay system is also depicted for comparison [20].

Figure 4.1 shows the secrecy outage probability of the relay systems versus

the density of eavesdroppers λ_e with various values of self-interference cancellation factor ρ for the transmit SNR $P/N_0 = 50, 60$ dB. It is shown that the analytical results perfectly match the simulation results. It is shown that as λ_e increases, the secrecy outage probability of the relay systems increases. It is also shown that the FD relay system has lower secrecy outage probability than the HD relay system for $\rho = -80, -60, -50$ dB when $P/N_0 = 50$ dB and for $\rho = -80, -60$ dB when $P/N_0 = 60$ dB.

Figure 4.2 shows the secrecy outage probability of the relay systems versus the self-interference cancellation factor ρ with various values of the density of eavesdroppers λ_e for the transmit SNR $P/N_0 = 60$ dB. It is shown that as ρ increases, the secrecy outage probability of the FD relay system increases. It is shown that the FD relay system has lower secrecy outage probability than the HD relay system for small values of ρ.

Figure 4.3 shows the secrecy outage probability of the FD relay system versus the transmit SNR P/N_0 with various values of the density of eavesdroppers λ_e for the self-interference cancellation factor $\rho = -80, -60$ dB. It is shown that as P/N_0 increases, the secrecy outage probability of the FD

relay system decreases until it reaches a minimum, and then increases. It is shown that as λ_e decreases, the optimal value of P/N_0 which minimizes the secrecy outage probability of the FD relay system decreases.

Figure 4.4 shows the secrecy outage probability of the FD relay system versus the transmit SNR P/N_0 with various values of the self-interference cancellation factor ρ for the density of eavesdroppers $\lambda_e = 10^{-4}$ m^{-2}. It is shown that as ρ decreases, the optimal value of P/N_0 which minimizes the secrecy outage probability of the FD relay system increases.

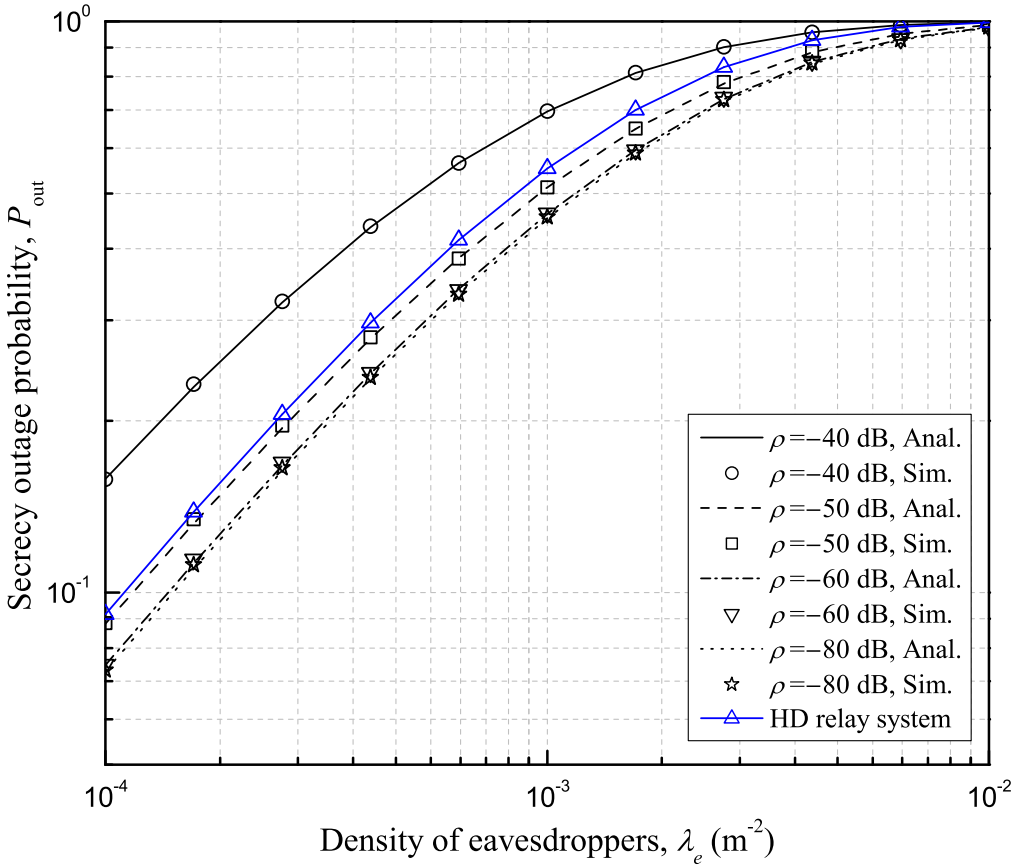
Figure 4.5 shows the average secrecy rate of the relay systems versus the density of eavesdroppers λ_e with various values of self-interference cancellation factor ρ for the transmit SNR $P/N_0 = 50, 60$ dB. It is shown that the analytical results perfectly match the simulation results. It is shown that as λ_e increases, the average secrecy rate of the relay systems decreases. It is shown that the FD relay system has higher average secrecy rate than the HD relay system for $\rho = -80, -60, -50$ dB.

Figure 4.6 shows the average secrecy rate of the relay systems versus the self-interference cancellation factor ρ with various values of density of

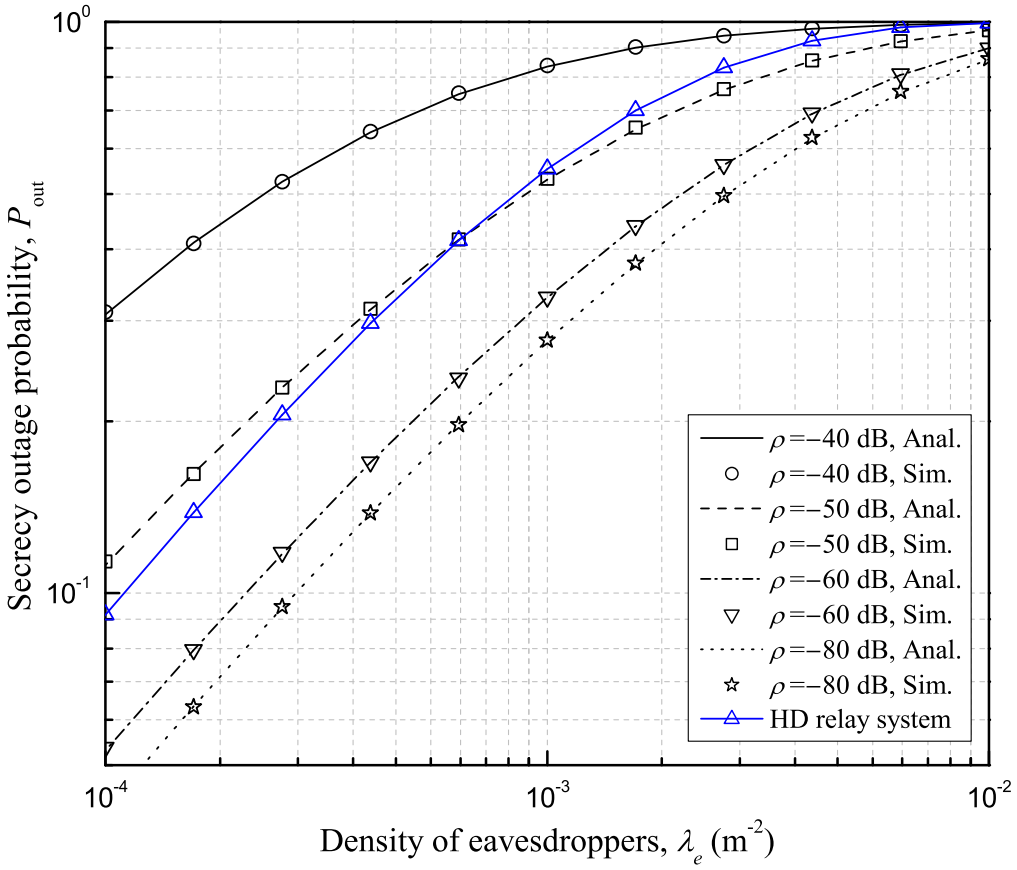
eavesdroppers λ_e for the transmit SNR $P/N_0 = 60$ dB. It is shown that as ρ increases, the average secrecy rate of the FD relay system decreases. It is shown that the FD relay system has higher average secrecy rate than the HD relay system for small values of ρ.

Figure 4.7 shows the average secrecy rate of the FD relay system versus the transmit SNR P/N_0 with various values of density of eavesdroppers λ_e for the self-interference cancellation factor $\rho = -80, -60$ dB. It is shown that as P/N_0 increases, the average secrecy rate of the FD relay system increases until it reaches a maximum, and then decreases.

Figure 4.8 shows the average secrecy rate of the FD relay system versus the transmit SNR P/N_0 with various values of the self-interference cancellation factor ρ for the density of eavesdroppers $\lambda_e = 10^{-4}$ m^{-2}. It is shown that as ρ decreases, the optimal value of P/N_0 which minimizes the average secrecy rate of the FD relay system increases.


10^0
10^{-1}
Secrecy outage probability, P_{out}
10^{-4}
10^{-3}
10^{-2}
Density of eavesdroppers, λ_e (m^{-2})
ρ=−40 dB, Anal.
ρ=−40 dB, Sim.
ρ=−50 dB, Anal.
ρ=−50 dB, Sim.
ρ=−60 dB, Anal.
ρ=−60 dB, Sim.
ρ=−80 dB, Anal.
ρ=−80 dB, Sim.
HD relay system

(a) $P/N_0 = 50$ dB



(b) $P/N_0 = 60$ dB

Figure 4.1. Secrecy outage probability versus density of eavesdroppers λ_e with various values of self-interference cancellation factor ρ.

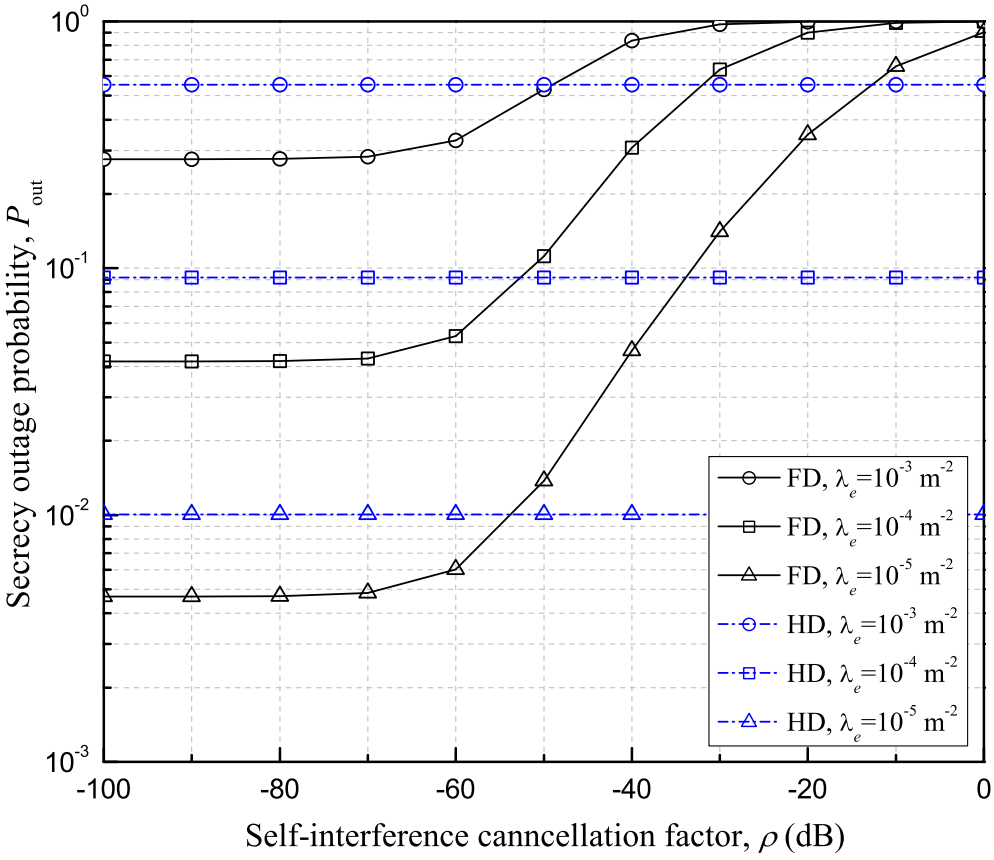
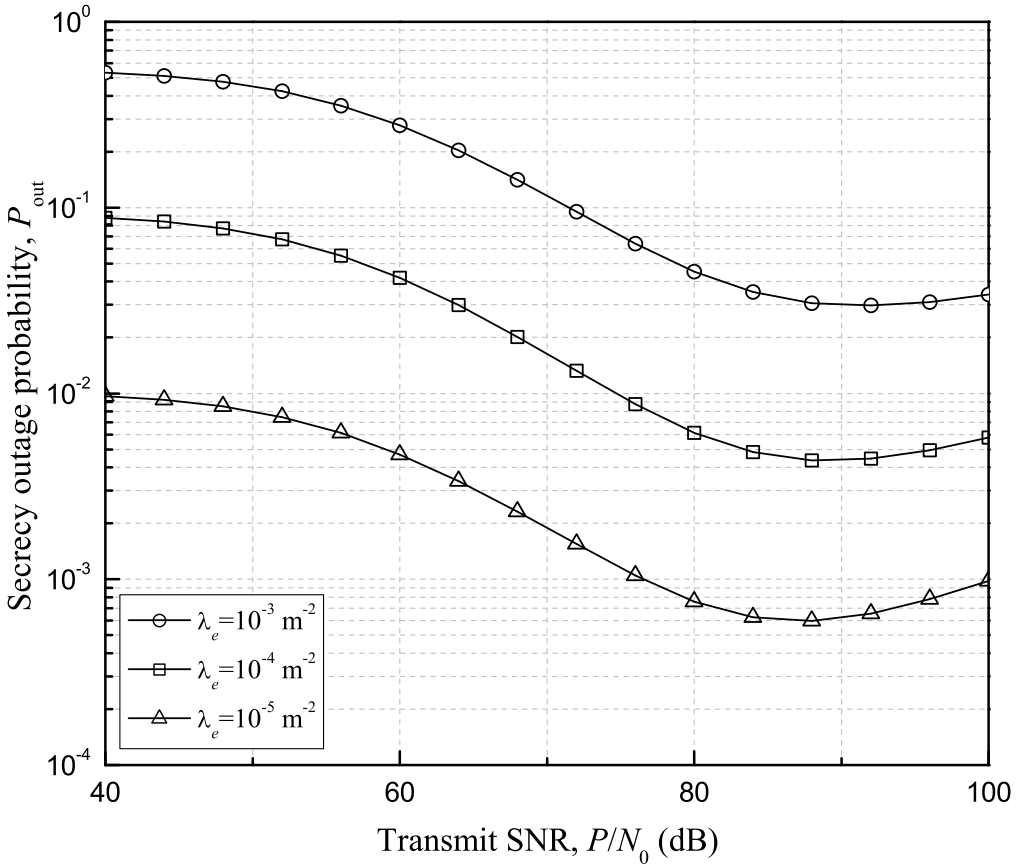
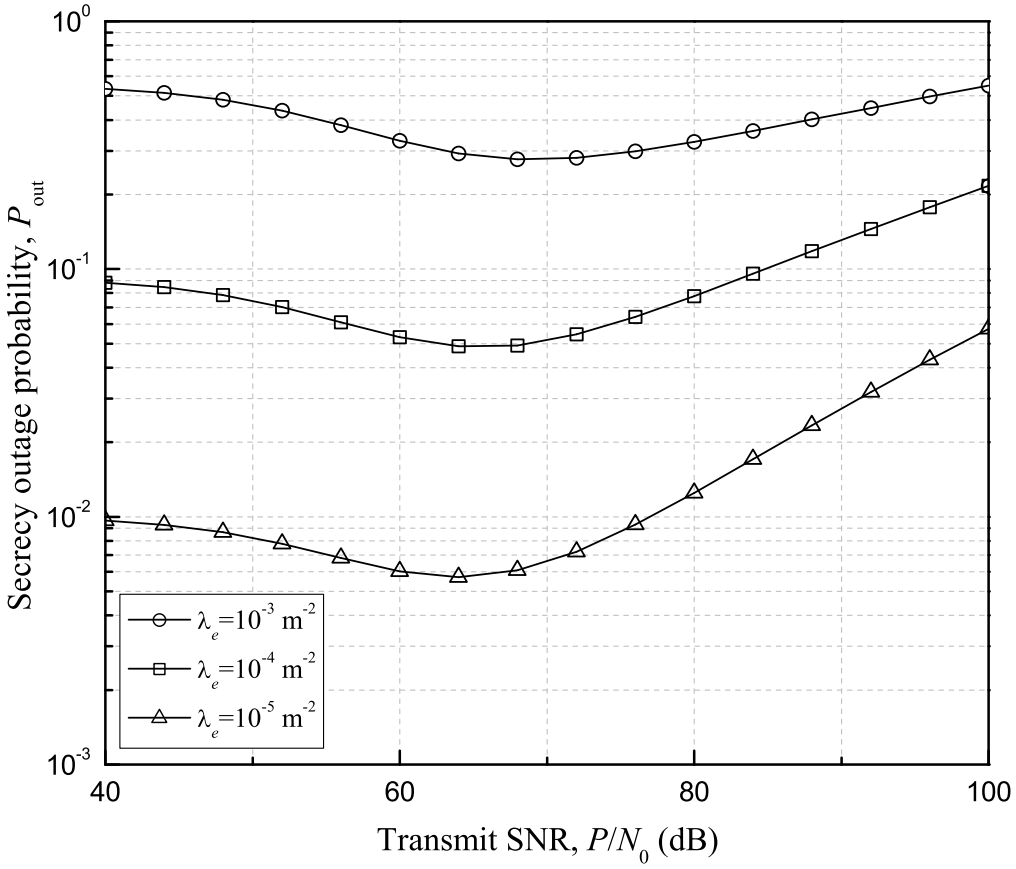


Figure 4.2. Secrecy outage probability versus self-interference cancellation factor ρ with various values of density of eavesdroppers λ_e.


Secrecy outage probability, P_{out}
Transmit SNR, P/N_0 (dB)
10^0
10^{-1}
10^{-2}
10^{-3}
10^{-4}
40
60
80
100
λ_e=10^{-3} m^{-2}
λ_e=10^{-4} m^{-2}
λ_e=10^{-5} m^{-2}

(a) $\rho = -80$ dB



(b) $\rho = -60$ dB

Figure 4.3. Secrecy outage probability versus transmit SNR P/N_0 with various values of density of eavesdroppers λ_e.

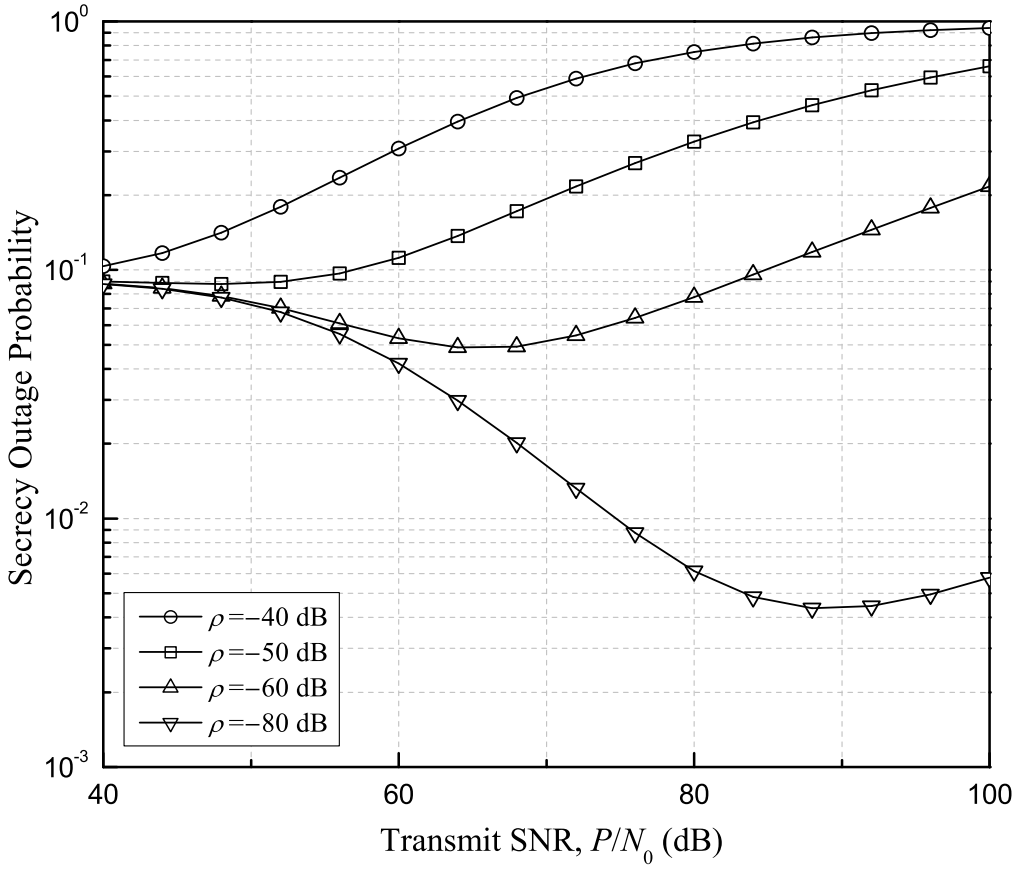
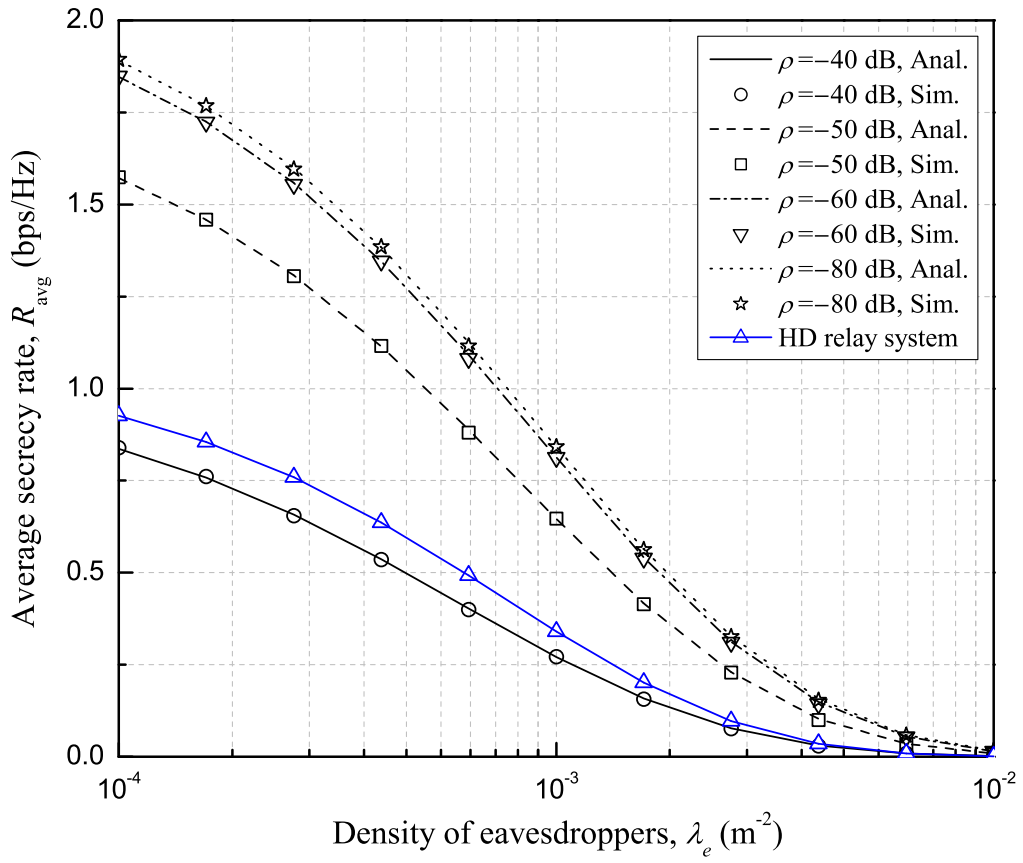
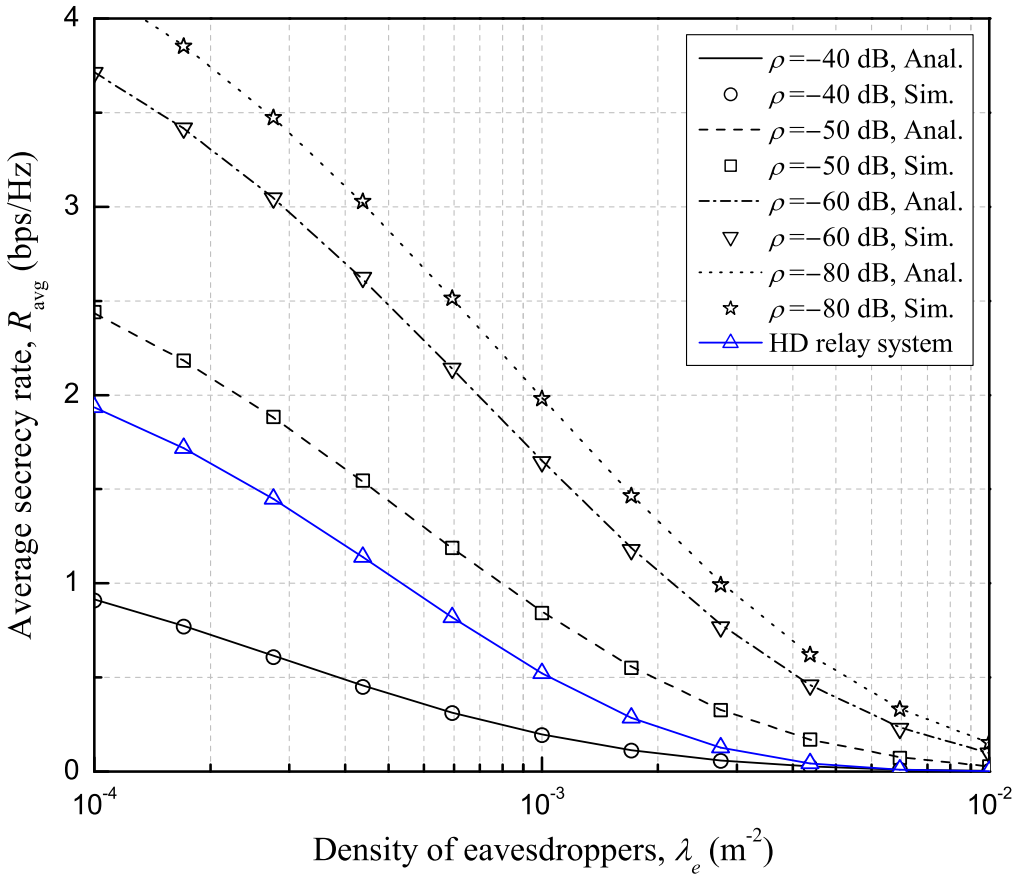


Figure 4.4. Secrecy outage probability versus transmit SNR P/N_0 with various values of self-interference cancellation factor ρ.


2.0
1.5
1.0
0.5
0.0
10^{-4}
10^{-3}
10^{-2}
Average secrecy rate, R_{avg} (bps/Hz)
Density of eavesdroppers, λ_e (m^{-2})
ρ=−40 dB, Anal.
ρ=−40 dB, Sim.
ρ=−50 dB, Anal.
ρ=−50 dB, Sim.
ρ=−60 dB, Anal.
ρ=−60 dB, Sim.
ρ=−80 dB, Anal.
ρ=−80 dB, Sim.
HD relay system

(a) $P/N_0 = 50$ dB



(b) $P/N_0 = 60$ dB

Figure 4.5. Average secrecy rate versus density of eavesdroppers λ_e with various values of self-interference cancellation factor ρ.

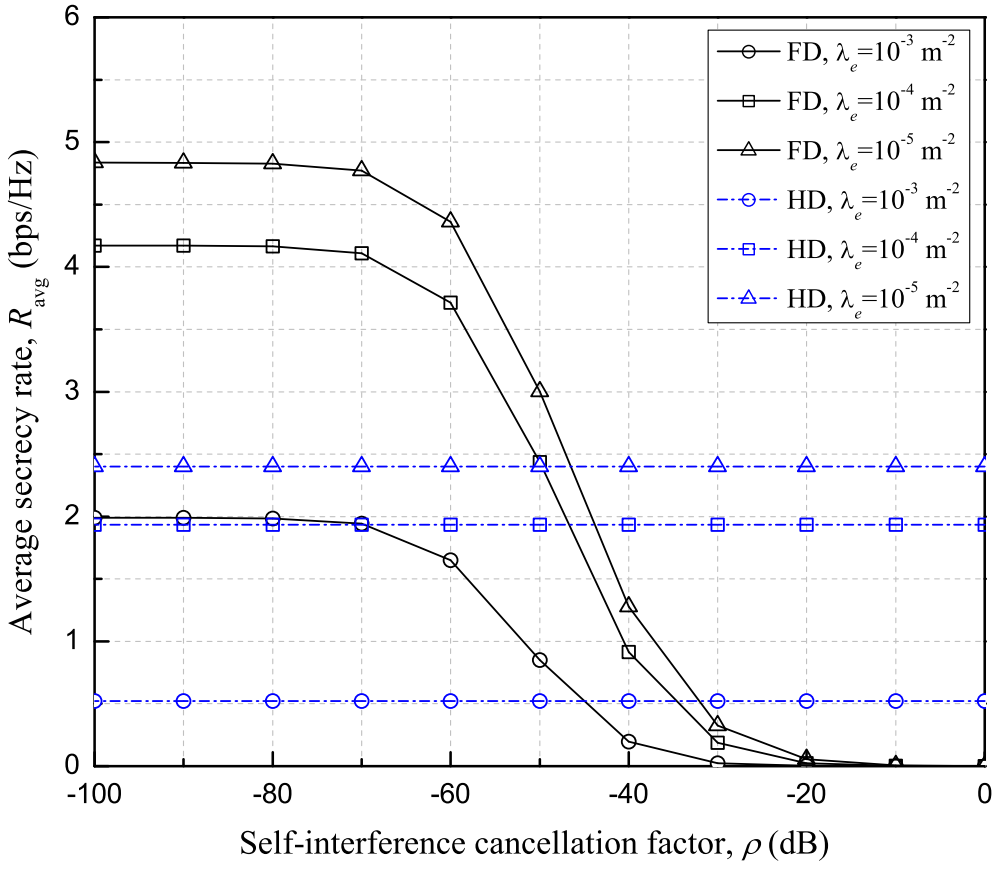
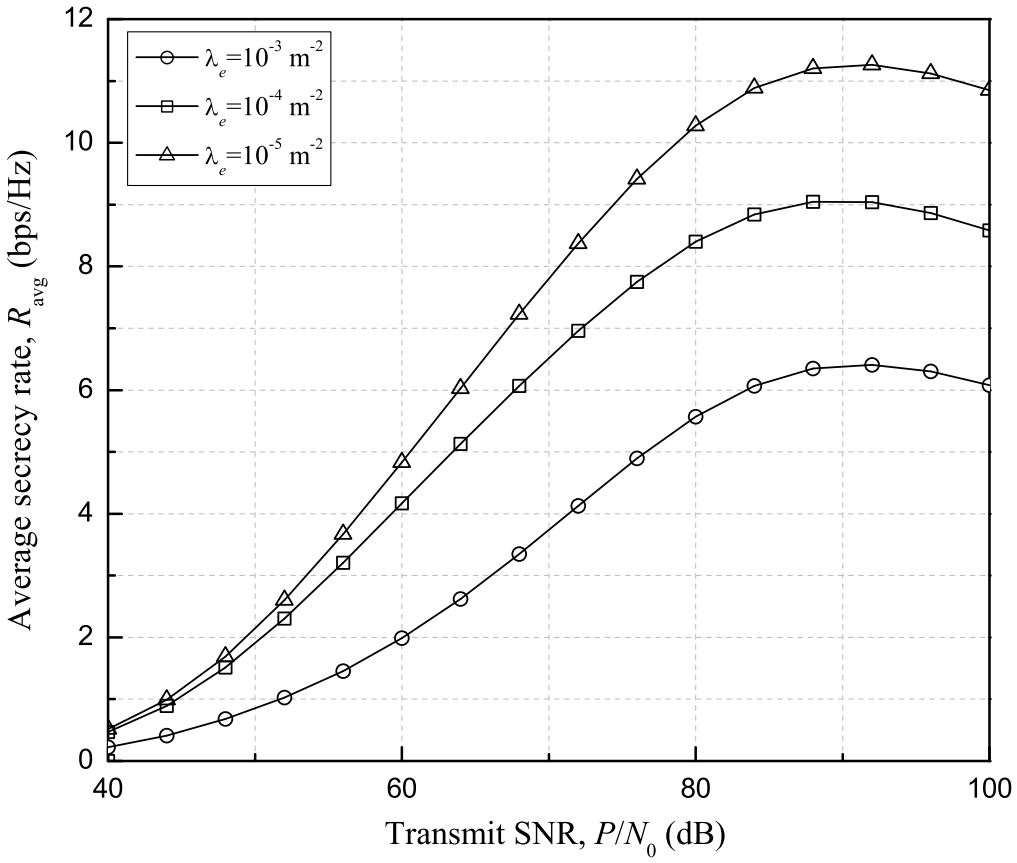
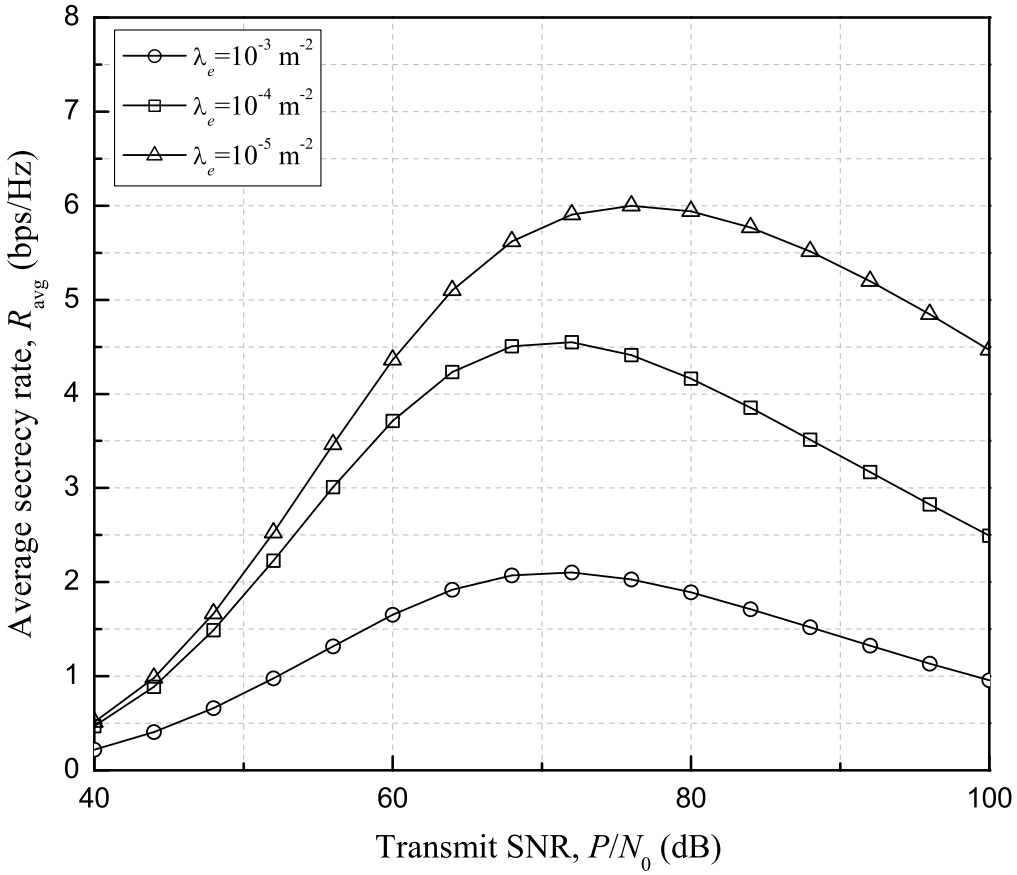


Figure 4.6. Average secrecy rate versus self-interference cancellation factor ρ with various values of density of eavesdroppers λ_e.


λe=10-3 m-2
λe=10-4 m-2
λe=10-5 m-2
Average secrecy rate, Ravg (bps/Hz)
Transmit SNR, P/N0 (dB)
0
2
4
6
8
10
12
40
60
80
100

(a) $\rho = -80$ dB



(b) $\rho = -60$ dB

Figure 4.7. Average secrecy rate versus transmit SNR P/N_0 with various values of density of eavesdroppers λ_e.

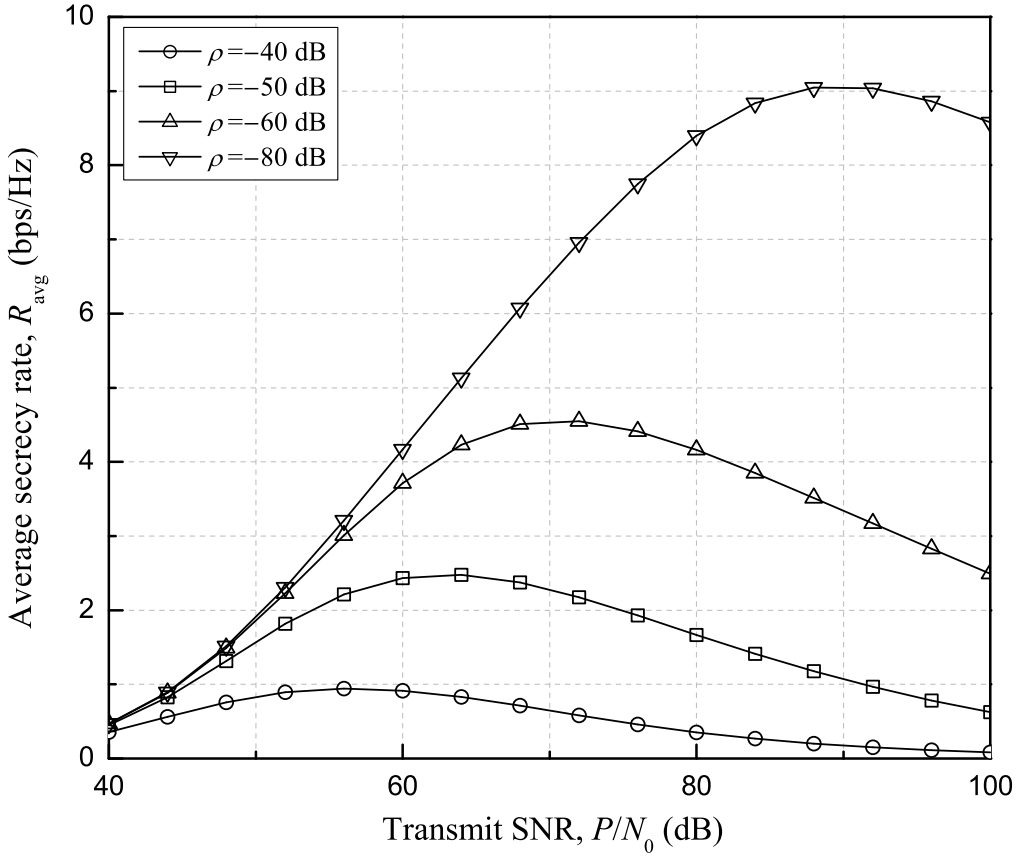


Figure 4.8. Average secrecy rate versus transmit SNR P/N_0 with various values of self-interference cancellation factor ρ.

Chapter 5

Conclusion

In this thesis, we consider a full-duplex (FD) relay system in the presence of randomly located eavesdroppers. We analyze the cumulative density functions of the end-to-end signal-to-interference-plus-noise ratio (SINR) from the source to the destination and the SINR at the most detrimental eavesdropper. We derive analytical expressions for the secrecy outage probability and the average secrecy rate of the system. Simulation results perfectly match the analytical results of the secrecy outage probability and the average secrecy rate. It is shown that the secrecy performance of the system is

improved as the density of eavesdroppers decreases. It is also shown that the FD relay system has higher secrecy performance than the half-duplex relay system when a large portion of self-interference is cancelled.

In our work, we suppose that each node in the FD relay system has a single antenna for analytical simplicity. To enhance secrecy performance of the FD relay system, a multi-antenna transmission scheme will be investigated where the source, the relay, and the destination have multiple antennas for transmitting information signals and generating artificial noises at the same time in our future work.

Bibliography

[1] H. Ju, E. Oh, and D. Hong, "Improving efficiency of resource usage in two-hop full duplex relay systems based on resource sharing and interference cancellation," *IEEE Trans. Wireless Commun.*, vol. 8, no. 8, pp. 3933-3938, Aug. 2009.

[2] E. Everett, A. Sahai, and A. Sabharwal, "Passive self-interference suppression for full-duplex infrastructure nodes," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 680-694, Feb. 2014.

[3] M. Duarte, C. Dick, and A. Sabharwal, Experiment-driven characterization of full-duplex wireless systems, *IEEE Trans. Wireless Commun.*, vol. 11, no. 12, pp. 42964307, Dec. 2012.

[4] B. Chun and Y. H. Lee, A spatial self-interference nullification method for full duplex amplify-and-forward MIMO relays, in *Proc. IEEE WCNC*, Apr. 2010, pp. 16.

[5] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless: Challenges and opportunities," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 9, pp. 1637-1652, Sep. 2014.

[6] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[7] C. E. Shannon, Communication theory of secrecy systems, *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656-715, Oct. 1949.

[8] G. Geraci, S. Singh, J. G. Andrews, J. Yuan, and I. B. Collings, "Secrecy rates in the broadcast channel with confidential messages and external eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 13, no. 5, pp. 2931-2943, May 2014.

[9] T.-X. Zheng, H.-M. Wang, J. Yuan, D. Towsley, and M. H. Lee, "Multi-antenna transmission with artificial noise against randomly distributed

eavesdroppers," *IEEE Trans. Commun.*, vol. 63, no. 11, pp. 4347-4362, Nov. 2015.

[10] G. Chen, J. P. Coon, and M. D. Renzo, "Secrecy outage analysis for downlink transmissions in the presence of randomly located eavesdroppers," *IEEE Trans. Inf. Forensics Security*, to be published.

[11] C. Liu, N. Yang, R. Malaney, and J. Yuan, "Artificial-noise-aided transmission in multi-antenna relay wiretap channels with spatially random eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7444-7456, Nov. 2016.

[12] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, "Physical layer security in downlink multi-antenna cellular networks," *IEEE Trans. Commun.*, vol. 62, no. 6, pp. 2006-2021, June 2014.

[13] Y. Deng, L. Wang, M. Elkashlan, A. Nallanathan, R. K. Mallik, and J. Yuan, "Physical layer security in three-tier wireless sensor networks: A stochastic geometry approach," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1128-1138, June 2016.

[14] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 574-583, Mar. 2015.

[15] S. Parsaeefard and T. Le-Ngoc, "Improving wireless secrecy rate via full-duplex relay-assisted protocols," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 10, pp. 2095-2107, Oct. 2015.

[16] B. Zhong and Z. Zhang, "Secure full-duplex two-way relaying networks with optimal relay selection," *IEEE Commun. Lett.*, to be published.

[17] Q. Li, W.-K. Ma, and D. Han, "Sum secrecy rate maximization for full-duplex two-way relay networks using Alamouti-based rank-two beamforming," *IEEE J. Sel. Signal Process.*, vol. 10, no. 8, pp. 1359-1374, Dec. 2016.

[18] D. Stoyan, W. Kendall, and J. Mecke, *Stochastic Geometry and Its Applications*, 2nd ed. New York, NY: Wiley, 1996.

[19] L. Wang, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Physical layer security of maximal ratio combining in two-wave with diffuse power

fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 2, pp. 247-258, Feb. 2014.

[20] C. Cai, Y. Cai, W. Yang, and W. Yang, "Secure connectivity using randomize-and-forward strategy in cooperative wireless networks," *IEEE Commun. Lett.*, vol. 17, no. 7, pp. 1340-1343, July 2013.

[21] X. Zhou, R. K. Ganti, J. G. Andrews, A. Hjrungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764-2775, Aug. 2011.

[22] T.-X. Zheng, H.-M. Wang, F. Liu, and M. H. Lee, "Outage constrained secrecy throughput maximization for DF relay networks," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1741-1755, May 2015.

[23] T.-X. Zheng, H.-M. Wang, F. Liu, and M. H. Lee, "Outage constrained secrecy throughput maximization for DF relay networks," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1741-1755, May 2015.

[24] J. Mo, M. Tao, and Y. Liu, "Relay placement for physical layer security: A secure connection perspective," *IEEE Commun. Lett.*, vol. 16, no. 6, pp. 878-881, June 2012.

[25] A. Kalantari, S. Maleki, G. Zheng, S. Chatzinotas, and B. Ottersten, "Joint power control in wiretap interference channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 3810-3823, July 2015.

[26] H. Alves, G. Brante, R. D. Souza, D. B. da Costa, and M. Latva-aho, "On the performance of secure full-duplex relaying under composite fading channels," *IEEE Signal Process. Lett.*, vol. 22, no. 7, pp. 867-870, July 2015.

[27] J. Huang and A. L. Swindlehurst, "Cooperative Jamming for Secure Communications in MIMO Relay Networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871-4884, Oct. 2011.

[28] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875-1888, Mar. 2010.

Korean Abstract

본 논문에서는 무작위로 위치한 다수 도청자가 존재할 때 복호 후 전송 전달 방식을 사용하는 전이중 중계기를 통해 송신기와 수신기가 통신하는 전이중 중계 시스템에 대해 연구한다. 송수신기 사이의 단대단 신호대간섭잡음비와 가장 해로운 도청자에서 신호대간섭잡음비의 누적분포함수를 유도하여 시스템의 보안 불능 확률과 평균 보안 전송률을 분석한다. 모의 실험을 통해 시스템의 보안 불능 확률과 평균 보안 전송률의 분석 결과가 실험 결과와 일치함을 확인한다.

주요어: 물리 계층 보안, 확률기하학, 전이중 중계 시스템, 무작위로 위치한 다수도청자, 보안 불능 확률, 평균 보안 전송률.

학번: 2015-20987.